JURISDICTIONAL EXPANSION BEYOND THE TERRITORY TO MITIGATE CONTEMPORARY TRANSNATIONAL CRIMES AND THE MANIPULATION OF ABUSIVE USE OF JURISDICTIONAL EXPANSION

M.S. Bhagya Veenaavi[1]

1. Introduction

Transnational crimes are defined by the necessary involvement of multiple jurisdictions. Transnational crimes operate across international borders and geographies. Such crimes affect states regardless of states' economic development or military strength. They involve illegal cross-border movements of people, goods and money. They lead to corruption and instability in governance. Moreover, transnational crimes frequently overlap with organized crimes. While organized crimes focus on structure and profitability, transnational crimes focus on cross-border jurisdictional dimensions of the criminal act.[2] But the distinction remains unclear in practice. The criteria of transnationality define the concept beyond mere physical location.[3] These indicate that crimes executed within the borders of one state have effects in other states. Their control needs international cooperation.

There is a disparity in how transnational crimes affect states. Large, hegemonic states have the power and the resources to control such crimes. They require technology, trained personnel and commitment of time and resources to control. Hegemonic states can also police transnational crimes if they are so inclined. But such states may also pose a danger in that they could use their power to impose their will on weaker states. They could ensure that their preferences are accepted as to how such crimes should be controlled. Less powerful states may have

---

[1] LL.B. (Reading), Department of Law, University of Jaffna. The author expresses her profound gratitude to Professor Muthucumaraswamy Sornarajah (Emeritus Professor of Law at the National University of Singapore) for his unwavering support, insightful advice and mentorship throughout this paper.

[2] UNODC, 'Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia' (September 2025) *Cybercrime Technical Brief Series*.

[3] Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 29 September 2003) 2225 UNTS 209 art 3(2)

to become beholden to the hegemonic state for the protection given. Extraterritorial power is both a sword and a shield.

2. Inadequacy of Territoriality, Particularly to Cybercrimes and Cybercrimes Affecting Climate Changes

These multi-billion-dollar networks of a wide range of illicit activities consist of crimes such as drug smuggling, arms and human trafficking, money laundering, corruption, counterfeit goods trafficking, trafficking in wildlife, natural resources, illegal waste dumping, and terrorism.[4] In present times, transnational crimes have changed form from these conventional forms to invisible, much more advanced forms. Specifically, globalization and digitization have transformed the landscape of transnational crimes by enabling these to expand their reach and increase efficiency.[5] Due to this, TNCs have become more complex. They thrive in an interconnected world. The convergence of the rise of global trade and financial liberalization with digital communication has made it easier for TNCs to move goods, money and people. The massive volume of global supply chains is being exploited to smuggle illicit goods like drugs and arms by hiding them within legitimate cargo. Furthermore, the rise of international banking allows criminals to easily launder money through shell companies and complex layering across different jurisdictions. The resulting economic disparities and vulnerable populations in certain regions offer TNCs a ready supply of victims for human trafficking and a labor pool for their enterprises. This broader nature of TNCs inadequate the territoriality to address TNCs effectively.[6]

Also, transnational crimes have posed a problem for the international community. While territoriality has been the basis for criminal jurisdiction, it is evident that the volume and sophistication involved in such crimes cannot be controlled by single states, especially developing

---

[4] UNEP and INTERPOL, *The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security* (2016) UNEP-INTERPOL Rapid Response Assessment.

[5] UNODC (n 2).

[6] Jean-Baptiste Maillart, 'The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime' (2018) *ERA Forum* <https://link.springer.com/article/10.1007/s12027-018-0527-2> accessed 23 December 2025.

states, which do not have the technology, the trained personnel and monetary resources necessary to control these crimes, which affect them disproportionately as they are easy targets. What has accentuated the problem is that new technology, particularly those associated with cyber activity, has immensely enhanced the capacity for the commission of such crimes. I take two such instances for special study: cybercrimes, specifically those involving the use of artificial intelligence and cybercrimes associated with climate change, which poses an immense threat to humanity. In both instances, the inadequacy of the territoriality principle is clear, and the need to explore other bases of jurisdiction is apparent.

3. Cybercrimes

Cyberspace, which was invented for the wellbeing of humans, has become a double-edged sword due to evolving cybercrimes. For example, end-to-end encryption technology ensures protected communication in digitalized world.[7] But this is being used by transnational criminals to network with international partners. The anonymity of the criminals is ensured through the exchange of cryptocurrencies. These strengthen the effect of TNCs while ensuring abusive use and harm to global supply chains. Most importantly, the globe cannot set aside digitization or globalization. Yet TNCs continue to adopt and create new means of crime beyond boundaries. Creation of new means does not deprive them of conventional platforms. At the end of the day, they have occupied new space while ensuring stability in conventional platforms, turning the condition much worse. For example, conventional fraud relied on human deception. But now financial crimes have intersected with AI, allowing for autonomous deepfake impersonations that bypass physical verification.

Cyberspace gives a more enclosed and anonymous floor, which boosts the sense of security by reducing risk to TNCs.[8] Cloud-based

[7] Jan Martijn Broekhof, 'What is end-to-end encryption and why is it important?' (Guardian360, 2023) https://guardian360.eu/what-is-end-to-end-encryption-and-why-is-it-important accessed 8 December 2025.

[8] Emile S. Mbungu Kala, 'Critical Role of Cyber Security in Global Economy' (2023) *Open Journal of Safety Science and Technology Vol.13 No.4.*

ransomware attacks are the best example of this.[9] In these attacks, the evidence is almost never in the same country. Instead of being in one file on one computer, information is broken into small pieces and spread across different servers all over the world; one piece is in Germany, another is in Brazil, another is in a cloud server that keeps moving its location. While the authorities are lawfully working to find out the evidence within their own borders, evidence is flying across the globe in seconds. By the time authorities get permission to ask another country for help, criminals have moved the data somewhere else. Though law has borders, cyberspace has no borders. Criminals can easily find a digital space to hide evidence that not even a powerful country can reach. So, a single attack can affect multiple jurisdictions. Cyber-crimes affect all with no deviation of gender, age, education, individual, group and gravity of the state power. Simply put, the boundaries between cyber and conventional crimes have disappeared, making the whole world vulnerable. Even the feelings and emotions of human subjects are exploited for profit and greed through dating and romance scams.

4. AI-related Cyber Crimes

Most importantly, the integration of AI has evolved a new landscape of cybercrimes. Transnational criminals adopt AI to expand their criminal operations. From autonomous cyberattacks and deepfake-enabled impersonation to AI-optimized malware and phishing campaigns, the malicious use of AI challenges personal liberty, national security and jurisdictional boundaries. For example, AI-generated code can be embedded into malware that adapts to its environment with no chance of detection. It could conceal malicious payloads within an application.[10] These are released only when the targeted victim is identified through geological or facial recognition. Importantly, this victim is not an individual anymore. It can be a state/states or a group of selected state entities physically located on one territory which works for another.

---

[9] Jan Kleijssen and Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options' in M Kuijer and W Werner (eds), *Netherlands Yearbook of International Law* 2016 (vol 47, TMC Asser Press 2017) 147.

[10] Harshith Kumar Pedarla, 'The Rise of AI-Generated Malware: Detection Challenges and Countermeasures' (2025) *11 International Journal of Information System and Innovative Technology 1* <https://doi.org/10.5281/zenodo.17426723 >

IBM's deep locker prototype is a good example.[11] AI-botnets are also another example. They are capable of scanning system vulnerabilities and bypassing verifications. This sustains high-volume spam, which could even break down highly secured systems. So, combating TNCs becomes a serious global challenge.

5. Cybercrimes Affecting Climate Changes

Cybercrimes also target climate change. When extreme weather causes physical damage to critical infrastructure, regulating authorities get distracted and become more vulnerable. Cybercriminals launch attacks such as ransomware and phishing scams targeting these weakened entities, causing further disruption, stealing data and extorting money. Moreover, cybercriminals exploit vulnerable populations by running fraudulent relief campaigns. Renewable energy sources and smart grids become targets of cyberattacks. This could result in the disruption of the power supply and cause blackouts. Greenwashing, hacktivism and supply chain attacks also taken place. Apart from climate change-associated cybercrimes, climate change-associated TNCs also have an impact on the global community.

Climate change fuels TNCs, and TNCs fuel climate change. This cyclic process, powered by the "profit-power oriented greed", finally declines the nature's ability to sequester and adapt to climate change impacts. Pathetically, this process neither knows boundaries nor jurisdictional limits. Impact is universal. Climate change is inherently linked with the loss of biodiversity and results in the degradation of ecosystems. In order to support nature's ability to mitigate climate change, integration of criminal justice systems addressing these crimes is important.[12]

Further, the nexus between TNCs and climate change questions the existence of sustainable development and world peace. Because, from my perspective, climate change-associated TNCs break down the world's security. A world without security facilitates no room for the mutual function of development goals and sustainable protection of the

[11] UNODC (n 2).

[12] UNODC and WWF, *Crimes that Affect the Environment and Climate Change* (Discussion Paper, 2021) 12.

environment. On the other hand, the nexus between TNCs and threat financing should be pointed out. Groups such as the Lord's Resistance Army and Janjaweed have been involved in the killings of elephants for ivory.[13] Currently, the trafficking of natural resources is one of the major revenue sources for transnational crimes. This again jeopardize global peace and security in terms of human and environment with no boundaries. Therefore, restoring global peace and security via the elimination of natural resources-based threat financing requires a borderless global movement.

I have identified the issues that need urgent attention. They involve global interests. My contention is that these issues can be dealt with through the adoption of extraterritoriality. Though it is true that extraterritorial jurisdiction is inherently obnoxious as it affects territorial sovereignty, exceptions must exist. I identify the areas that I have indicated as areas in which the use of extraterritoriality is justified. I will explain this view further.

6. The Need for Extraterritoriality

At the point of sorting out the required global movement in the existing context, "jurisdiction" should be reconsidered. Out of different principles of jurisdiction in international law, territoriality is fundamental. The principle of territoriality depends on two assumptions: physical location, which is observable and verifiable.[14] But based on the current nature of TNCs, the first question I would raise is, "Are we able to point out a physical location for TNCs?". TNCs have evolved into a ubiquitous state which inherently transcends geographical boundaries. On the other hand, there is a view that the concept of territoriality is interconnected with democratic governance. Democratic governing derives its power from the people within its boundaries. As TNCs operate outside these walls, the rulers lose the ability to effectively impose laws. Because TNCs can move their digital

[13] UNEP and INTERPOL, *The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security* (2016) UNEP-INTERPOL Rapid Response Assessment.

[14] Muthucumaraswamy Sornarajah, 'Theorising Extraterritorial Jurisdiction: The Travails of TWAIL' (2024) *35(2) National Law School of India Review 32.*

hands without moving a single person, thereby effectively escaping from democratic control. Further, TNCs extract massive value from citizens and nature. But the state cannot effectively regulate TNCs because their operations transcend the territory and territoriality. This highlights the insufficiency of territoriality to manipulate the impact of TNCs over their own territory.

As well, even though jurisdiction is territorial, subjects intended to be regulated under law are not territorial anymore. Modern threats routinely transcend geographical boundaries and cannot be effectively solved by a single national jurisdiction. The rise of complex cross-border crimes such as cybercrime, human trafficking, nexus of organized crime and terrorism financing and serious international war crimes exposes limitations of the territorial approach, necessitating international cooperation to prevent impunity. "Operation SpecTor",[15] which shut down the dark Web market platform monopoly, can be raised as an example from the real world.

In my perspective, existing context and necessities call for extraterritoriality to be involved in the manipulation of contemporary TNCs. Yet, it is considered obnoxious. Because it affects sovereignty and can be intrusive, in that a powerful state can control events in other states. However, the gradual increase of TNCs necessitates a reduction in hostility to extraterritoriality in specific areas. Simply, immense economic power, which exceeds the GDP of many states and the political power of TNCs, operates as a de-spatialized network, making them difficult to regulate under territorial jurisdiction. This leads to an exploitation of gaps between territorially bound national laws and international agreements, especially those in the global south with weak enforcement capacity.

---

[15] Orlaith Traynor, 'Dark Web Takedowns in 2023 | An Overview for CISOs'(CybelAngel, 22 January 2024) <https://cybelangel.com/blog/the-main-dark-web-takedowns-of-2023-an-overview-for-cisos/#:~:text=3:%20Monopoly%20Market%20What%20did%20this%20marketplace,countries%20from%20inside%20and%20outside%20the%20EU> accessed 9 December 2025.

Extraterritoriality, which is my suggestion for the mitigation of TNCs, is currently resented by most of the global community. Capitulation regimes experience that the world experienced in the past is one of the major reasons for TWAIL to rescind extraterritoriality from their end.[16] But it should be highlighted that we live in a context which is far from the history where capitulation regimes and opium wars used to define extraterritoriality. Currently, extraterritoriality means the exercise of jurisdiction on the events taking place in another state for the effect caused on one's own territory. This execution firstly violates the sovereignty of the other state. Secondly, it paves the way for the creation of hegemony. Part of the world interprets this as a new form of imperialism. Further, they argue that this opens the floor for legal imperialism as well.[17] While acknowledging the potential credibility of this argument, I would highlight that this execution of power is not absolute. Genealogical analysis proves that the historic powers, specifically the European, used extraterritoriality to earn capital and make their authoritative presence over other weak states. But in the current context, states are reluctant to use these sorts of modes as recognition of their own acts by the global community matters. They nowadays use diplomatic modes—such as cultural diplomacy and gastro diplomacy—to make their presence in other states. Then, they start to influence internal affairs through their very diplomatic presence. My point is that, though the world rescinded extraterritoriality to prevent new modes of imperialism, it finds its own ways to exist. At the end of the day, what we lose is the ability to mitigate TNCs before they become worse.

One of the major objections to the expansion of extraterritoriality is the notion of self-determination.[18] Claim to avoid the application of extraterritoriality because it violates the right to self-determination is not credible. Because in exceptional situations like transnational crimes, the common good should be prioritized over self-determination.

---

[16] Muthucumaraswamy Sornarajah (n 14).

[17] BS Chimni, 'The international law of jurisdiction: A TWAIL perspective' (2022) *35 Leiden Journal of International Law 29.*

[18] Evan J Criddle, 'Extraterritoriality's Empire: How Self-Determination Limits Extraterritorial Lawmaking' (2024) *118 American Journal of International Law 607.*

Extraterritoriality is often rejected as offending principles like self-determination, but must be permissible in situations of new crimes that affect global interests, or when the state exercising it is doing good to the affected country, as in cyber-crimes, where that country, lacking resources and personnel, cannot control. The USA indictment and effort against the North Korean "Lazarus" group for the 2016 Bangladesh bank heist can be raised as an example for this. This attack targeted the global financial system via the SWIFT network, attempting to steal nearly one billion dollars and successfully diverting eighty-one million out of this. At the material time, as the crime affected global financial stability, involving multi-jurisdictional traces that a less-resourced nation like Bangladesh could not adequately manage alone, the USA authorities asserted extraterritorial jurisdiction. This demonstrates that a powerful state's actions are implicitly justified by the need to protect the integrity of the international financial system when traditional territorial law enforcement is insufficient.

The obnoxious features of extraterritoriality do not apply to certain crimes which affect the international community as a whole. Most such crimes are subject to universal jurisdiction. But some crimes are new and are not included in this list. Such crimes, like those associated with climate change, can only be dealt with through extraterritoriality.

I would argue that when a state uses extraterritoriality in situations I have identified above, it acts to the benefit of the global community and has the tacit consent of the states that are affected by the exercise of extraterritorial jurisdiction, as they are given protection from transnational crimes at no cost. This gets over any objection based on self-determination, for if the citizens of a state benefiting from the protection against TNCs are asked, they would agree that their state should consent to the use of extraterritoriality.

7. Conclusion

While I argue for the expansion of extraterritoriality to mitigate TNCs, I do acknowledge that the potential for misuse comes along with this. Yet there are possible benefits that can result from expansion. For example, strengthening extraterritoriality ensures justice for those who need it most. Yet power-oriented greed can block the way to justice. So,

in my perspective, the globe should be capable of striking a balance between these two ends, rather than setting aside extraterritoriality. In order to do this, theory and reality ought to be bridged. Then, a realistic set of checks and balances should be established to checkmate state parties that seek hegemony or any individual who gains when it is time to give foremost place to the common good of the globe.